UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

KORRI WYNN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

LABORATORY SERVICES COOPERATIVE,

Defendant.

Case No. 25-cv-00762

CLASS ACTION COMPLAINT

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

TABLE OF CONTENTS

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

I. NATURE OF THE ACTION

1. Plaintiff Korri Wynn ("Plaintiff" or "Plaintiff Wynn") brings this class action against Defendant Laboratory Services Cooperative ("LSC" or "Defendant") for its failure to properly secure and safeguard the protected health information ("PHI") and personally identifiable information ("PII") (collectively, "Private Information") of Plaintiff and other similarly situated patients of LSC ("Class members").

2. Defendant collected and maintained the Private Information of the proposed Class members who are patients of LSC, including individuals who visited certain Planned Parenthood centers.

3. Defendant owed a non-delegable duty to Plaintiff and Class members to implement reasonable and adequate cyber-security measures to protect their Private Information.

4. Failing to implement reasonable and adequate cyber-security measures has significant consequences for the patients and employees whose records are unlawfully accessed by cyber-criminals and identity thieves.

5. On or around October 27, 2024, the Private Information of Plaintiff and Class members was targeted, compromised and unlawfully accessed by cyber-criminals in a data breach (the "Data Breach"). Upon information and belief, cyber-criminals hacked into Defendant's computer systems and obtained the Private Information of approximately 1,600,000 individuals. Defendant has stated that the Data Breach affected select Planned Parenthood centers that receive lab testing services from LSC. The Private Information compromised in the breach includes Plaintiff's and Class members' names, addresses, phone numbers, emails, date(s) of service, diagnoses, treatment, medical record number, lab results, patient/accession number, provider name, treatment location, related-care details, health insurance plan name, health insurance plan type, health insurance member/group ID numbers, billing details, bank account details, billing codes, payment card details, balance details, social security numbers, driver's

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

license or state ID numbers, passport numbers, dates of birth, demographic data, student ID number, and other forms of government identifiers.[1]

6. This preventable Data Breach occurred because of Defendant's failure to implement adequate and reasonable cyber-security measures to ensure its computer systems were protected. Because Defendant's data security protocols and practices were deficient, unauthorized actors were able to access, acquire, appropriate, encumber, exfiltrate, steal, use, and/or view Plaintiff's and Class members' Private Information.

7. The Private Information compromised in the Data Breach was obtained by cyber-criminals and remains in their possession, where it is valuable to identity thieves.

8. As a result of the Data Breach, Plaintiff and Class members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which upon information and belief: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect that Private Information.

9. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been subject to unauthorized access by an unknown third party and precisely what specific type of information was accessed.

[1] Laboratory Services Cooperative, *Notice of Data Breach* (Apr. 10, 2025), https://www.lscincidentsupport.com/.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

10. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and stolen during the Data Breach.

11. Plaintiff and Class members have a continuing interest in ensuring that their Private Information is properly safeguarded, and are entitled to injunctive and other equitable relief.

II. PARTIES

12. Plaintiff Korri Wynn is a citizen of the State of Maryland, and a resident of Baltimore County, Maryland.

13. Defendant LSC is a Washington non-profit corporation with a registered address of 2001 East Madison Street, Seattle, WA 98122.

III. JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

15. This Court has personal jurisdiction over Defendant because it is registered to do business, and maintains its principal place of business, in Seattle, Washington.

16. Venue is proper in in this District pursuant to 28 U.S.C. § 1391(b) because Defendant is headquartered in this District, and a substantial part of the acts or omissions giving rise to this action occurred in this District.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

IV. ADDITIONAL FACTUAL ALLEGATIONS

A. Defendant Acquires, Collects, and Maintains Plaintiff's and Class members' Private Information

17. Defendant is a non-profit organization based in Seattle, which provides lab testing services to certain Planned Parenthood centers in 30 states as well as the District of Columbia.[2] Defendant has a total annual revenue of approximately $18 million dollars. [3]

18. As part of its regular course of business, Defendant collected the highly sensitive Private Information of patients, including Plaintiff and Class members.

19. Upon information and belief, as part of its regular course of business, Defendant thereafter maintained and stored Plaintiff's and Class members' Private Information on its systems.

20. Upon information and belief, while collecting the Private Information of Plaintiff and Class members, Defendant agreed to provide confidentiality and adequate security for the data that it collected through its internal policies and through other disclosures in compliance with statutory privacy requirements.

21. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

B. The Data Breach and Defendant's Failure to Adequately Disclose Same

22. On or around October 27, 2024, Defendant identified suspicious activity within its network and became aware that it was subject to a cyber-security attack. Following an investigation that concluded in February 2025, Defendant confirmed that an unauthorized actor had breached its computer systems and compromised its network.

23. Despite identifying the breach on October 27, 2024, and concluding its investigation into the breach in February 2025, Defendant did not post notice on its website

[2] Steve Alder, *Laboratory Services Cooperative Breach Impacts 1.65 Million People*, THE HIPAA JOURNAL (Apr. 11, 2025), https://www.hipaajournal.com/laboratory-services-cooperative-data-breach/.

[3] https://projects.propublica.org/nonprofits/organizations/263813271 (last accessed April 23, 2025).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

("Website Notice") or begin to file notices with state attorneys general offices until April 10, 2025, over five months after it identified the breach.

24. Defendant's website notice, published on April 10, 2025 ("Website Notice"), explained that:

> On October 27, 2024, LSC identified suspicious activity within its network. In response, LSC immediately engaged third-party cybersecurity specialists to determine the nature and scope of the incident and notified federal law enforcement. The investigation revealed that an unauthorized third party gained access to portions of LSC's network and accessed/removed certain files belonging to LSC.[4]

25. Defendant's Website Notice was wholly inadequate, lacking vital information such as how the unauthorized actor(s) gained access to its networks, when the Data Breach actually occurred (as opposed to when it was discovered by LSC), whether the accessed data was encrypted or otherwise protected, the duration of the breach, how it was discovered, the specific Planned Parenthood Centers in select states that partner with LSC, and why impacted individuals were not notified that their information was compromised until more than five months after the breach was discovered.

26. The Data Breach occurred because Defendant did not implement adequate and reasonable cyber-security procedures and protocols to protect the Private Information of Plaintiff and Class members. Because Defendant's data security protocols and practices were deficient, unauthorized person(s) were able to access, view, and/or exfiltrate Plaintiff's and Class members' Private Information.

27. Plaintiff further believes that her Private Information and that of Class members may have been subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cyber-criminals that commit cyber-attacks of this type.

C. Defendant's Data Breach Was Imminently Foreseeable and Preventable

28. Despite the growing body of publicly available information regarding the rise of ransomware attacks and other forms of cyber-attacks that compromise Private Information,

[4] *Notice of Data Breach*, *supra* note 1.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

Defendant's approach to maintaining the privacy of Plaintiff's and Class members' Private Information was inadequate, unreasonable, negligent, and reckless. This is evidenced by Defendant's acknowledgment that since the breach it has "implemented several measures to further enhance the security of its environment" including "new and updated risk analysis to stay vigilant against ongoing threats, performing additional vulnerability testing and penetration testing, and providing additional security training for employees."[5]

29. As a laboratory services provider to select Planned Parenthood centers, LSC should have been aware that the data stored on its systems was a likely target for cyber-criminals. Just months before the Data Breach, in August 2024, Planned Parenthood of Montana experienced a security incident affecting over 18,000 individuals.[6] Additionally, in late 2021, Planned Parenthood Los Angeles was also the subject of a ransomware attack that exposed the personal information of approximately 400,000 patients.[7]

30. Moreover, as an entity in the healthcare industry, Defendant should have been aware of the industry's ongoing struggle to address increasingly sophisticated cyberattacks. In 2023, the healthcare sector experienced its worst year on record for cyberattacks, with 725 reported incidents and more than 124 million health records breached.[8]

31. In light of the largest healthcare breaches of 2023, including but not limited to HCA Healthcare (11,270,000 individuals affected), Perry Johnson & Associates, Inc. (8,952,212 individuals affected), Managed Care of North America (8,861,076 individuals affected), Welltok, Inc. (8,493,379 individuals affected), HealthEC LLC (4,452,782 individuals affected), and Reventics, LLC (4,212,823 individuals affected), Defendant knew or should have known

---

[5] *Id.*

[6] Steve Alder, *Planned Parenthood Ransomware Attack Affects 18,000 Patients*, THE HIPAA JOURNAL (Nov. 8, 2024), https://www.hipaajournal.com/planned-parenthood-ransomware-2024/.

[7] Lawrence Abrams, *Planned Parenthood LA discloses data breach after ransomware attack*, BLEEPINGCOMPUTER (Dec. 1, 2021), https://www.bleepingcomputer.com/news/security/planned-parenthood-la-discloses-data-breach-after-ransomware-attack/.

[8] Steve Alder, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (Jan. 31, 2024), https://www.hipaajournal.com/security-breaches-in-healthcare/.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

that the Private Information it collected and maintained would be a prime target for cybercriminals.[9]

32. It is well known that Private Information, including Social Security numbers and health related information, are extremely valuable commodities and a frequent, intentional target of cyber-criminals. Companies that collect such information, including Defendant, are or should be well aware of the risk of being targeted by cyber-criminals.

33. To mitigate the heightened risk of data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by the United States Government:

- **Implement an awareness and training program:** Educate employees and individuals about the threat of ransomware and how it is delivered, as end users are often the primary targets.
- **Enable strong spam filters:** Prevent phishing emails from reaching end users by using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to block email spoofing.
- **Scan all incoming and outgoing emails:** Detect threats by scanning emails and filtering executable files to prevent them from reaching end users.
- **Configure firewalls:** Block access to known malicious IP addresses to prevent unauthorized access.
- **Patch operating systems, software, and firmware:** Regularly update and patch devices, potentially using a centralized patch management system for greater efficiency.
- **Set anti-virus and anti-malware programs for regular scans:** Ensure these programs run automatic scans to detect and remove potential threats.
- **Manage privileged accounts based on the principle of least privilege:** Limit administrative access to users only when absolutely necessary and ensure those with admin privileges use them only when required. Implement an awareness and training program.
- **Configure access controls:** Implement least privilege principles for file, directory, and network share permissions. Users should only have access to what they need—

[9] *76 HIPAA Breach Report Statistics for 2023,* https://www.paubox.com/blog/76-hipaa-breach-report-statistics-for-2023 (last accessed April 23, 2025).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

if a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- **Disable macro scripts in office files transmitted via email:** Prevent the execution of potentially harmful macros by disabling them in office files sent via email. Consider using Office Viewer software instead of full office suite applications to open email attachments.

- **Implement Software Restriction Policies (SRP):** Use SRPs or similar controls to prevent programs from executing from common ransomware locations, such as temporary folders associated with web browsers or compression programs, including the AppData/LocalAppData folder.

- **Disable Remote Desktop Protocol (RDP):** If RDP is not in use, consider disabling it to reduce potential attack vectors.

- **Use application whitelisting:** Allow only programs that are explicitly permitted by security policy to execute, blocking any unauthorized or potentially malicious software.

- **Execute operating system environments or specific programs in a virtualized environment:** Run sensitive systems or programs in isolated virtual environments to reduce risk.

- **Categorize data based on organizational value:** Implement physical and logical separation of networks and data for different organizational units to protect critical information and ensure appropriate access control.[10]

34. To mitigate the heightened risk of data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by Microsoft's 2023 Digital Defense Report:

- **Enable multifactor authentication (MFA)**. This protects against compromised user passwords and helps to provide extra resilience for identifies.

- **Apply Zero Trust principles.** This includes ensuring users and devices are in a good state before allowing access to resources, allowing only the privilege that is needed for access to a resource and no more, assuming system defenses have been breached and systems may be compromised.

- **Use extended detection and response (XDR) and antimalware**. Implement software to detect and automatically block attacks and provide insights into the security operations software.

[10] *How to Protect Your Networks from Ransomware: Technical Guidance Document*, https://www.justice.gov/criminal/criminal-ccips/file/872771/dl (last accessed April 23, 2025).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

- **Keep up to date**. Unpatched out-of-date systems are a key reason many organizations fall victim to cyber-attacks.

- **Protect data**. Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.[11]

35. Defendant also could and should have implemented the following preventive measures, as recommended by the Federal Trade Commission ("FTC") in its latest update to *Protecting Personal Information: A Guide for Business*:

- Know what personal information you have in your files and on your computers.
- Keep only what you need for your business.
- Protect the information that you keep.
- Properly dispose of information you no longer need.
- Create a plan to respond to security incidents.[12]

36. Defendant could and should have implemented the following additional preventive measures, as recommended by the Joint Ransomware Task Force's ("JRTF") #StopRansomware Guide, although this list does not encompass the full range of recommended actions:

- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface.

- **Regularly patch and update software and operating systems to the latest available versions.** Prioritize timely patching of internet-facing servers-that operate software for processing internet data such as web browsers, browser plugins, and document readers-especially for known exploited vulnerabilities….

- **Create, maintain, and regularly exercise a basic cyber incident response plan (IRP) and associated communications plan that includes response and notification procedures**. For example, providing data breach notifications to third parties and regulators consistent with law.

- **Limit the use of RDP and other remote desktop services.** If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through

[11] Microsoft Threat Intelligence, *Microsoft Digital Defense Report: Building and improving cyber resilience* (Oct. 2023), available at https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[12] FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client.

- **Ensure all on-premises, cloud services, mobile, and personal devices are properly configured, and security features are enabled**. For example, disable ports and protocols that are not being used for business purposes.[13]

37. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class members as a result of a breach.

38. Despite widespread reports of data breaches, Defendant neglected to implement the necessary safeguards to ensure the Private Information of Plaintiff and Class members was protected.

39. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially hundreds of thousands of individuals' Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the data.

40. Given the volume and sensitivity of the Private Information belonging to Plaintiff and Class members stored on its systems, Defendant could—and should—have implemented all of the above measures to prevent and detect cyberattacks.

41. The occurrence of the Data Breach indicates that Defendant failed to implement one or more of the above measures to prevent cyber-security attacks. The failure to implement some or all of the above measures resulted in the Data Breach and the exposure of approximately 1.6 million Class members' Private Information.

D. Plaintiff's and Class members' Private Information Has Significant Value

42. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying

[13] Cybersecurity & Infrastructure Security Agency, *#StopRansomware Guide* (rev. Oct. 19, 2023), available at https://www.cisa.gov/resources-tools/resources/stopransomware-guide.

[14] 17 C.F.R. § 248.201.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

43. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[16]

44. The data compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information at the point-of-sale in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

45. Unauthorized access to an individual's medical records and/or health related records can have serious consequences. Stolen medical records can be stored for long periods, with individuals often remaining unaware that their records have been compromised or stolen.[17] Moreover, the monetary value of medical records on the dark web far exceeds that of credit card numbers. For example, the cyber-security firm Trustwave discovered that medical records can fetch up to $250 per record on the dark web, while credit card numbers typically sell for around $5 each.[18]

46. Medical records are highly valuable to cyber-criminals, not only because of the price they can be sold for on the dark web, but also due to the various ways they can be exploited. Cyber-criminals can use stolen medical records to commit medical identity theft to submit fraudulent medical claims, purchase prescriptions, or receive unauthorized treatment.

---

[15] *Id.*

[16] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.

[17] iFax, *The Value of Protected Health Information (PHI) To Hackers: Understanding the Risks and Implications*, https://www.ifaxapp.com/hipaa/phi-hackers-risks-implications/ (last accessed April 23, 2025).

[18] Trustwave, *2018 Trustwave Global Security Report*, https://trustwave.azureedge.net/media/15350/2018-trustwave-global-security-report-prt.pdf?rnd=131992184400000000 (last accessed April 23, 2025).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

These actions pose significant threats and risks to patients whose medical information has been compromised, leading to potential financial, physical, and emotional harm.

47. According to the FTC, if a hacker or an individual to whom the hacker sells your medical information mixes it with your own, it could impact the medical care you receive, or the health insurance benefits available to you. The FTC's Medical Identity Theft Frequently Asked Questions highlight several red flags victims should watch for, including: (i) receiving bills for medical services they didn't receive, (ii) being contacted by debt collectors about medical debt they don't owe, (iii) seeing unrecognized medical collection notices on their credit report, (iv) spotting incorrect office visits or treatments on their explanation of benefits, (v) being informed by their health plan that they've reached their benefits limit, or (vi) being denied insurance because their medical records reflect a condition they do not have.[19]

48. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

49. Plaintiff and Class members now face years of constant surveillance of their personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

[19] FTC, *Medical Identity Theft: FAWs for Health Care Providers and Health Plans* (Jan. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

[20] U.S. Gov't Accountability Office, Report to Congressional Requesters, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identify Theft Is Limited; However, the Full Extent Is Unknown* at 29 (June 2007), available at https://www.gao.gov/assets/gao-07-737.pdf.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

E. Defendant Failed to Comply with FTC Guidelines

50. Defendant was also prohibited by the FTCA (15 U.S.C. § 45), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has determined that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal information constitutes an "unfair practice" in violation of the Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

51. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

52. For example, in 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines advise businesses, *inter alia*, to protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[21]

53. The guidelines further advise businesses: not to maintain PII longer than necessary for authorization of a transaction; to limit access to sensitive data; to use an intrusion detection system to expose a breach as soon as it occurs; to monitor all incoming traffic for activity indicating someone is attempting to hack the system; to watch for large amounts of data being transmitted from the system; and to verify that third-party service providers have implemented reasonable security measures.[22]

54. To underscore the binding significance and legal ramifications of the promulgated guidance, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or

[21] *Protecting Personal Information*, *supra* note 12.

[22] *Id.*

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

practice prohibited by Section 5 of FTCA, 15 U.S.C. § 45.[23] Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices.

56. Upon information and belief, Defendant was at all times fully aware of its obligations to protect the Private Information of Plaintiff and Class members, and Defendant was also aware of the significant repercussions that would result from its failure to do so.

57. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information, or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. Defendant Failed to Comply with HIPAA.

58. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (45 C.F.R. § 160.102) and as such was required to protect against reasonably anticipated threats to the security of Private Information in its systems. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[24]

59. Title II of HIPAA contains what are known as the Administrative Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

---

[23] *See, e.g.*, *FTC*, 799 F.3d at 236 (determining that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal information constitutes an "unfair practice" in violation of the Act).

[24] The HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?*, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last accessed April 23, 2025).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

60. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*;

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

i. Failing to effectively train all members of its workforce (including agents and independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

61. At all times, Defendant was fully aware of its responsibilities under HIPAA to safeguard individuals' private information, yet it failed to meet these obligations. Defendant also understood the serious consequences that would arise from its failure to comply. Given the nature and volume of the private information it collected and stored, as well as the foreseeable damages that could result, Defendant's actions were particularly egregious.

G. Defendant Failed to Comply with Industry Standards.

62. Cybersecurity experts routinely identify companies, particularly healthcare providers and their business associates, in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

63. In light of the evident threat of cyberattacks seeking Private Information held by companies, like Defendant, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by companies, like Defendant, in possession of individuals' Private Information, including but not limited to: educating and training all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data; monitoring and limiting network ports; and protecting web browsers and email management systems. Defendant failed to follow these industry best practices.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

64. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

65. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

66. These foregoing frameworks are existing and applicable industry standards for large companies, and upon information and belief, Defendant failed to comply with these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

H. Common Injuries & Damages

67. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class members has materialized and is imminent, and Plaintiff and Class members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which upon information and belief: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

68. The ramifications of Defendant's failure to safeguard the Private Information of Plaintiff and Class members are long-lasting and severe. In 2023 alone, American adults lost $43 billion to identity theft.[25] Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

I. The Data Breach Increases Victims' Risk of Identity Theft and Fraud

69. The unencrypted Private Information of Class members will likely end up for sale on the dark web as that is the *modus operandi* of hackers.

70. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members as a result of the Data Breach.

71. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

72. Plaintiff's and Class members' Private Information is of great value to hackers and cyber-criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit off their misfortune.

73. Further, the standard operating procedure for cyber-criminals is to use some data, like the Private Information here, to access and/or develop "fullz packages" of that person.[26]

---

[25] Christina Inazito, *Identity Fraud Cost Americans $43 Billion in 2023*, AARP (Apr. 10, 2024), https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html.

[26] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

74. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

75. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a comprehensive Fullz package and sell it—and then resell it in perpetuity—at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

J. Loss of Time to Mitigate Risk of Identity Theft and Fraud

76. Cyber-attacks and data breaches like the Data Breach are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

77. GAO released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[27]

78. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

---

cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See* Uri Brison, *'Fullz', 'Dumps', and more: Here's what hackes are selling on the black market*, VENTUREBEAT (Feb. 8, 2015), https://venturebeat.com/security/fullz-dumps-and-cvvs-heres-what-hackers-are-selling-on-the-black-market/.

[27] U.S. GAO, *supra* note 20.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

79. Plaintiff and Class members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, contacting credit bureaus to place freezes on their credit and checking their financial accounts. Accordingly, the Data Breach has caused Plaintiff and Class members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

80. These efforts are consistent with the GAO Report in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

81. Plaintiff's mitigation efforts are consistent with the GAO Report and with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing and/or correcting their credit reports, contacting companies to remove fraudulent charges from their accounts, and placing a credit freeze on their credit.[29]

K. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

82. Based on the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for various forms of identity theft crimes.

83. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the

[28] *See* id.

[29] *See* Fed. Trade Comm'n, *IdentityTheft.gov*, https://www.identitytheft.gov/Steps. (last accessed Apr. 23, 2025).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

84. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

85. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from Defendant's Data Breach.

L. Plaintiff Wynn's Experience

86. Plaintiff is not sure how LSC received her Private Information but believes her Private Information was provided to LSC by Planned Parenthood, where she received services.

87. LSC provides lab testing services to Planned Parenthood.

88. Upon information and belief, at the time of the Data Breach, Defendant maintained Plaintiff Wynn's Private Information on its system.

89. On information and belief, Plaintiff Wynn's Private Information was compromised in the Data Breach and stolen by cyber-criminals who illegally accessed Defendant's network for the purpose of specifically targeting Private Information.

90. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent self-monitoring her accounts to ensure no fraudulent activity has occurred.

91. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from potential identity theft. Plaintiff fears for her personal financial security due to the uncertainty over the Private Information that was exposed in the Data Breach and the individuals who may have access to it as a result of the Data Breach.

92. As a result of the Data Breach, Plaintiff Wynn has suffered loss of time, interference, and inconvenience. Plaintiff Wynn has also experienced increased concern for the loss of her privacy.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

V. CLASS ALLEGATIONS

93. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

94. The Class that Plaintiff seeks to represent is defined as follows:

> All United States citizens whose Private Information was compromised as a result of the Data Breach disclosed by LSC on or around April 10, 2025.

95. Excluded from the Class are Defendant and its officers; directors and employees; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

96. Plaintiff reserves the right to modify and/or amend the Class, including, but not limited to, creating additional subclasses as necessary.

97. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

98. All Class members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class members, which can be used for providing notice to Class members.

99. This action has been brought and may be properly maintained on behalf of the Class and proposed herein under Federal Rule of Civil Procedure 23.

100. ***Numerosity.*** Consistent with Fed. R. Civ. P. 23(a)(l), the Class are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes millions of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records. Reportedly, the Data Breach included approximately 1,600,000 individuals.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

101. ***Commonality and Predominance.*** Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class members. Such common questions include:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant violated the FTCA and HIPAA;

c. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class members;

d. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

e. Whether Defendant had duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

f. Whether Defendant failed to adequately safeguard Plaintiff's and Class members' Private Information;

g. Whether and when Defendant actually learned of the Data Breach;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their Private Information had been compromised;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their Private Information had been compromised;

j. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

l. Whether Plaintiff and Class members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and the Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

102. ***Typicality.*** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of the claims of other Class members in that Plaintiff, like all Class members, had her personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class members were injured through the misconduct of Defendant and assert the same claims for relief.

103. ***Adequacy of Representation.*** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Plaintiff is a member of the Class she seeks to represent; is committed to pursuing this matter against Defendant to obtain relief for the Class; and has no interests that are antagonistic to, or in conflict with, the interests of other Class members. Plaintiff retained counsel who are competent and experienced in litigating class actions and complex litigation, including data breach litigation of this kind. Plaintiff and her counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

104. ***Superiority.*** Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class members have been harmed by Defendant's wrongful conduct and/or action. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

105. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the common questions of law or fact predominate over any questions affecting Plaintiff or any individual Class members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

106. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(l) because the prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. By contrast, conducting this litigation as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class members would create the risk of adjudications with respect to individual Class members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

107. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to Plaintiff and the Class as a whole, making injunctive and declaratory relief appropriate to Plaintiff and the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retain possession of Plaintiff's and Class members' Private Information, and has not been forced to change its practices or to relinquish Private Information by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

108. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present discrete common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Plaintiff's and Class members' Private Information was accessed, compromised, or stolen in the Data Breach;

b. whether Defendant owed a legal duty to Plaintiff and Class members;

c. whether Defendant failed to adequately monitor its data security systems;

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

d. whether Defendant failed to take adequate and reasonable steps to safeguard the Private Information of Plaintiff and Class members;

e. whether Defendant failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Defendant knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiff's and Class members' Private Information secure; and

g. whether Defendant's adherence to FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach

109. Lastly, all members of the proposed Class are readily ascertainable. LSC has access to Class members' names and addresses affected by the Data Breach.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

110. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 109, as if fully set forth herein.

111. Defendant collected, stored, and maintained the Private Information of Plaintiff and Class members as part of the regular course of its business operations, which services affect commerce.

112. Defendant knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiff and the Class and the importance of adequate security.

113. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

114. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

duty of care to use reasonable means to secure and safeguard its computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duties included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

115. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

116. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the Private Information.

117. Defendant's duty to implement reasonable security measures stems from common law, as well as regulations under the FTC Act and HIPAA, both of which require the Defendant to use appropriate cyber-security measures.

118. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

119. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class members of the Data Breach.

120. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

121. Defendant breached its duties, pursuant to the FTCA, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

Plaintiff's and Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of its networks and systems;
- Allowing unauthorized access to Class members' Private Information;
- Failing to detect in a timely manner that Class members' Private Information had been compromised;
- Failing to remove the Private Information of individuals it formerly engaged with when it was no longer required to retain that information pursuant to regulations; and
- Failing to timely and adequately notify Class members about the Data Breach's occurrence and scope, so that they could take appropriate action to mitigate the potential for identity theft and other damages.

122. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class members.

123. Plaintiff and Class members were within the class of persons the FTCA and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

124. Defendant's violation of the FTCA and HIPAA also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiff and the proposed Class members from the harms associated with data breaches.

125. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

126. Defendant has admitted that the Private Information of Plaintiff and Class members was wrongfully disclosed to unauthorized third persons because of the Data Breach.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

127. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class members, the Private Information of Plaintiff and Class members would not have been compromised.

128. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

129. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in Defendant's industry and the industries Defendant supports.

130. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems or transmitted through third party systems.

131. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

132. Plaintiff and the Class had no ability to protect their Private Information that was in, and is believed to remain in, Defendant's possession.

133. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

134. Neither Plaintiff nor Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

135. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

136. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed by unauthorized third parties as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

137. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

138. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

139. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf Of Plaintiff and the Class)

140. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 109 as if fully set forth herein.

141. Defendant entered into one or more written contracts with Planned Parenthood to provide lab testing services.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

142. Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and Class members and to timely and adequately notify them of any Data Breach.

143. These contracts were made expressly for the benefit of Plaintiff and Class members, as Plaintiff and Class members were the intended third-party beneficiaries of the contracts entered into between Defendant and Planned Parenthood. Defendant knew that, if it were to breach these contracts with Planned Parenthood, Planned Parenthood's patients, Plaintiff and Class members would be harmed.

144. Defendant breached the contracts it entered into with Planned Parenthood by, among other things, (i) failing to use reasonable data security measures, (ii) failing to implement adequate protocols and employee training sufficient to protect Plaintiff's and Class members' Private Information from unauthorized disclosure to third parties, and (iii) failing to promptly and adequately notify Plaintiff and Class members of the Data Breach.

145. Plaintiff and the Class were harmed by Defendant's breach of its contracts with Planned Parenthood, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result of Defendant's breach.

COUNT III
WASHINGTON DATA BREACH NOTIFICATION LAW
RCW 19.255.010, *et seq.*
(On behalf of Plaintiff and the Class)

146. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 109, as if fully set forth herein.

147. LSC, as an entity that facilitates and/or takes responsibility for the collection, handling, dissemination, and other dealings with nonpublic Private Information (as defined in RCW 19.255.005(2)(a)), is subject to the notice requirements of RCW 19.255.010(1).

148. Plaintiff and the Class members' Private Information includes "Private Information" as defined by RCW 19.255.005(2)(a).

149. In accordance with Washington law, LSC, as a business that owns, licenses, or maintains computerized data that includes "Private Information," was required to accurately

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

notify Plaintiff and the Class of the Data Breach affecting its data security systems if Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay pursuant to RCW 19.255.010(1),(2).

150. The Data Breach described herein constituted a "breach of the security of the system" of LSC as defined by RCW 19.255.005(1).

151. Because LSC knew and/or reasonably believed that Plaintiff's and Class members' Private Information was acquired by unauthorized persons during the Data Breach, LSC had an obligation to disclose the Data Breach in a timely and accurate fashion.

152. Upon information and belief, as a proximate result of LSC's failures to maintain its data security systems, Plaintiff's and Class members' Private Information was not secured and was accessed or compromised by cyber-criminals during the Data Breach.

153. As alleged above, LSC unreasonably delayed informing Plaintiff and the Class members about the Data Breach, affecting their Private Information, after LSC knew that the Data Breach had occurred.

154. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, LSC violated RCW 19.255.010(1),(2).

155. As a result of LSC's violation of RCW 19.255.010(1), (2), Plaintiff and the Class members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and the Class because their stolen Private Information would have had less value to identity thieves.

156. As a result of LSC's violation of RCW 19.255.010(1), (2), Plaintiff and the Class suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

157. As a direct and proximate result of LSC's violation of RCW 19.255.010(1), (2) Plaintiff and the Class suffered damages, as described above.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

158. Plaintiff and the Class seek relief under RCW 19.255.010(1), (2) for the harm they suffered due to LSC's willful violations of RCW 19.255.040(3)(a)(b), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT IV
WASHINGTON CONSUMER PROTECTION ACT
RCW 19.86.020, *et seq.*
(On behalf of Plaintiff and the Class)

159. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 109, as if fully set forth herein.

160. LSC is a "person" as defined by RCW 19.86.010(1).

161. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by RCW 19.86.010(2).

162. LSC engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of RCW 19.86.020, including, but not limited to:

a. Failing to implement and maintain reasonable security and privacy measures with regard to its data security systems in order to protect Plaintiff's and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks which were a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Failing to timely and adequately notify Plaintiff and the Class of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that it did not

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

reasonably or adequately secure Plaintiff's and Class members' Private Information; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

163. LSC's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LSC's data security practices and the ability of LSC to protect the confidentiality of consumers' Private Information.

164. LSC acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff's and Class members' rights. Given LSC's affiliation with Planned Parenthood—an organization that has recently suffered two separate data breaches—as well as its ties to the broader healthcare system, LSC was put on notice that its data security and privacy protections were insufficient.

165. LSC's conduct is injurious to the public interest because it violates RCW 19.86.020, a statute that contains a specific legislative declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the Washington residents affected by the Data Breach.

166. As a direct and proximate result of LSC's unfair and deceptive acts and practices, Plaintiff and the Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

167. Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law to recover actual damages sustained by each Class member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiff, on behalf of herself and Class members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

increase the damages award for each Class member by three times the actual damages sustained, not to exceed $25,000.00 per Class member.

COUNT V
INVASION OF PRIVACY
(On behalf of Plaintiff and the Class)

168. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 109, as if fully set forth herein.

169. Plaintiff and Class members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

170. Defendant owed a duty to Plaintiff and Class members to keep their Private Information confidential.

171. Defendant affirmatively and recklessly disclosed Plaintiff's and Class members' Private Information to unauthorized third parties.

172. The unauthorized disclosure and/or acquisition by a third party of Plaintiff's and Class members' Private Information is highly offensive to a reasonable person.

173. Defendant's reckless and negligent failure to protect Plaintiff's and Class members' Private Information constitutes an intentional interference with Plaintiff's and the Class members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

174. In failing to protect Plaintiff's and Class members' Private Information, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

175. Because Defendant failed to properly safeguard Plaintiff's and Class members' Private Information, Defendant had notice of and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

176. Defendant knowingly did not notify Plaintiff and Class members in a timely fashion about the Data Breach.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

177. As a proximate result of Defendant's acts and omissions, Plaintiff's and the Class members' sensitive Private Information was stolen by a third party and is now likely available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

178. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

179. Plaintiff and Class members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff's and the Class members' Private Information.

180. Plaintiff, on behalf of herself and Class members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. For an Order certifying the Class and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members;

c. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class members;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

d. For an award of damages, including actual, nominal, consequential, and punitive damages, as allowed by law in an amount to be

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: April 24, 2025.

s/ Steve W. Berman
Steve W. Berman, WSBA #12536
HAGENS BERMAN SOBOL SHAPIRO LLP
1301 Second Avenue, Suite 2000
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com

/s/ Lori G. Feldman
Lori G. Feldman, WSBA #29096
GEORGE FELDMAN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
lfeldman@4-justice.com
eservice@4-justice.com